Wireless Emergency Stop System

User's Manual

Rugged Remote Emergency Stop System with Reliable, Low Latency Wireless and Simple Integration Interface

HRI's Wireless Emergency Stop System is a medium to long-range wireless controller designed from the ground up to enable the safe operation of remote and automated systems. It provides a rugged, ergonomic, and easy to use control of safety equipment in industrial, construction, mining, or military applications. Both the handheld and receiver implement HRI's proprietary SafetySense™ technology to ensure consistent and reliable control.

1. Applications

- Safe control of remote dangerous equipment where human intervention may be needed.

2. Key Features (Wireless Emergency Stop – WES-001)

- SafetySense™ Secure wireless communications with AES128 encryption and range of 1000+ ft.
  - Frequency bands include 900 MHz, 2.4 GHz (Other bands available)
- Guaranteed low latency emergency stop response
- 1000+ unique system addresses
- 12 hour battery life for continuous use
- Flexible USB charging interface
- RP-SMA antenna connector
- IP65 rated enclosure
- Designed to meet MIL-STD-810 for ruggedness
- -20°C to 60°C operation (Extended temperature options available)
- Belt clip and lanyard options

3. Key Features (Safety Controller – VSC-012/VSC-013)

- SafetySense™ Secure wireless communications and range of 1000+ ft.
  - Frequency bands include 900 MHz, 2.4 GHz (Other bands available)
- USB, RS-232 serial, and CAN bus support for flexible system integration options
- Hardware-based SafetySense™ implementation for high reliability, no single point of failure safety implementation
- Differential wired emergency stop input
- Master enable outputs for direct stop of motion control equipment
- 8 to 32 VDC power input

- USB configuration for programming and configuration
- Multiple connector options available
  - RP-SMA antenna connector
  - Mini-CPC 4 pin for USB
  - Mini-CPC 9 pin for Power, Estop I/O, RS232, and CAN interfaces
  - 30p Hirose DF-13 (VSC-013 OEM only)
- IP66 (NEMA 4X) rated enclosure (VSC-012 only)
- -20°C to 60°C operation (Extended temperature options available)
- ROS™ and C drivers available to accelerate system software development for advanced applications

4. SafetySense™ Technology

SafetySense™ Technology consists of four major system-level technologies that work together to provide the integrator the ability to design systems with consistent and reliable remote operations.

4.1. System-Level Monitoring

All communication links in the system are designed requiring positive feedback. These heartbeat messages are sent on each link in the system (remote to receiver and receiver to integrator computer) at a rate of 50 Hz. This ensures that any fault in the link between the receiver and remote or integrator computer can be quickly detected.

4.2. Hardware Health Monitoring

While the receiver is monitoring the health of both the remote and the user computer, it contains dedicated hardware that is monitoring its internal health. Both firmware-based and independent hardware based watchdog timers monitor the functionality of the receiver firmware. The communication link to the remote is also monitored directly in hardware (independent of the firmware-based monitoring). Finally, the reference clock source, used by this custom hardware block, is monitored by a third independent timer to ensure that is operating within its specifications. A failure in any of these components causes the system to indicate an emergency stop situation.

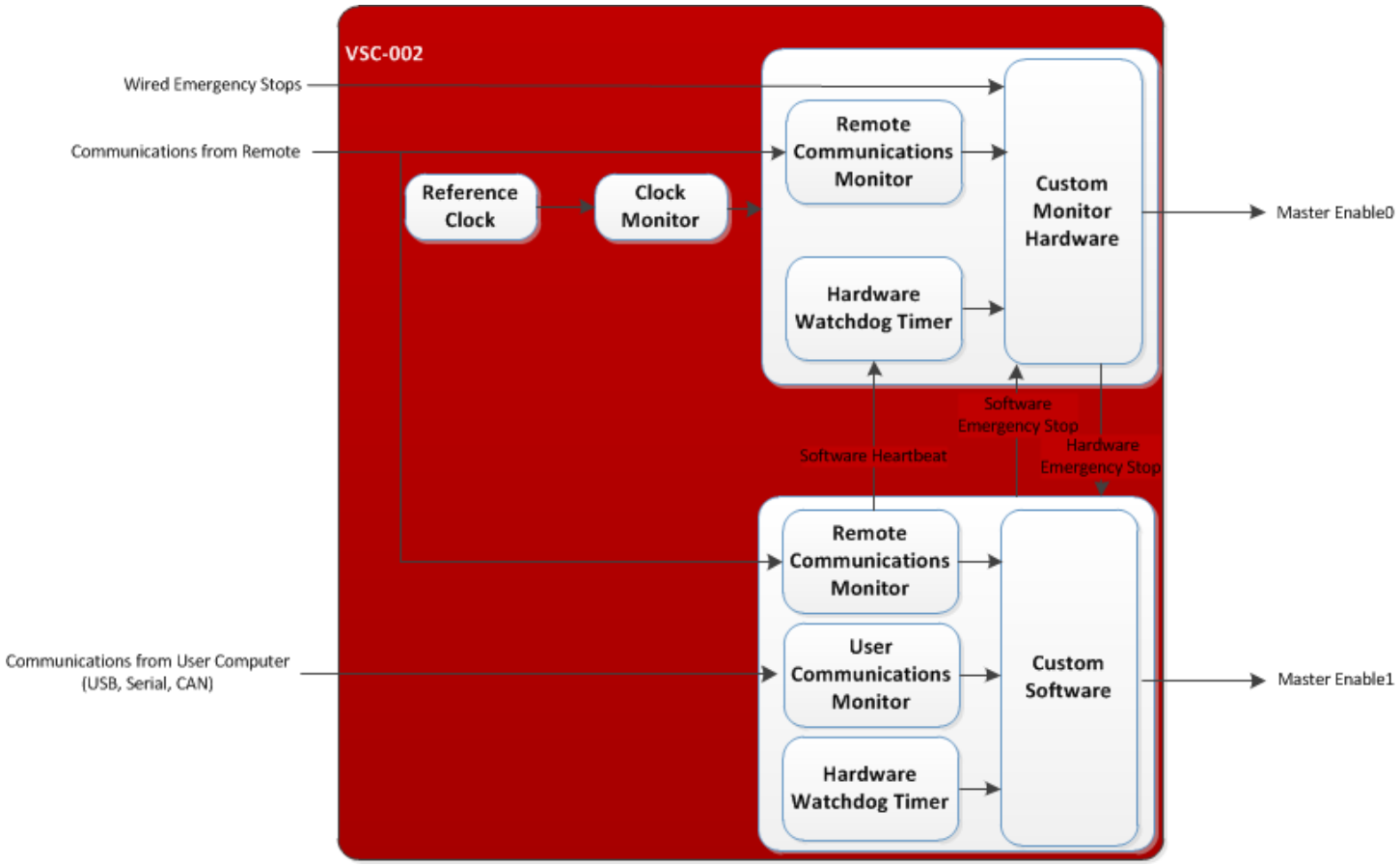

Figure 1 - Internal Hardware Monitors

The figure above illustrates the internal structure of the VSC. It is designed from the ground up to ensure that no single point of failure (hardware or software) exists that could cause an unsafe condition to not be caught and indicated by the Master Enable outputs. It is important that system designers pay careful attention in the integration of the VSC with their drive system to ensure that motion will be prevented when the Master Enable signals are de-asserted.

4.3. Consistent User Intervention

While the system is constantly monitoring its health, the remote also provides the operator with the ability to intervene. The WES's dedicated emergency stop button causes the receiver to indicate an emergency stop in a maximum of 500ms (absolute worst case). This, along with wired emergency stop buttons, gives the system designer significant flexibility.

5. Typical Integration Methods

5.1. WES Wireless Integration

Typically, the WES is integrated as a simple receiver where the VSC is connected to a pair of safety relays that control energy to the system. An example of this type of integration is shown below.

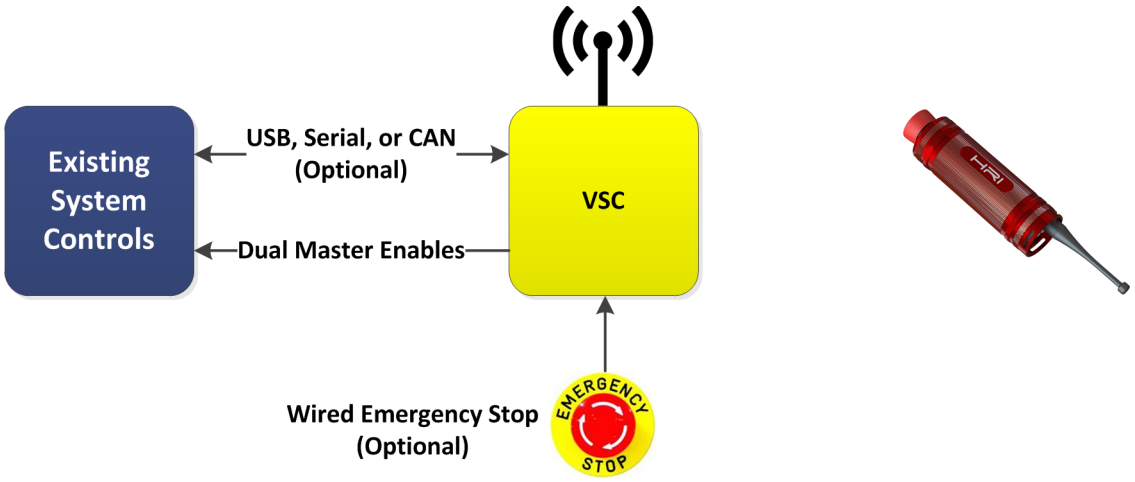

Figure 2 - Simple Receiver Integration

The VSC's integration interfaces allow for more sophisticated monitoring and management of the emergency stop network.

6. Operation

The VSC provides an Emergency Stop interface for hardware based emergency control as well as two Master Enable (normally high, low asserted) outputs. If the Emergency Stop input is activated, the Master Enable signals are asserted immediately by VSC hardware. All command and control communication to the VSC is over the USB, RS232, or CAN-based interfaces. The specific protocols for each are defined in detail below.

The Wireless Emergency Stop System has three modes while operating: Searching, Stopped, and Operational. The basic features of these modes are summarized in Table 1.

Mode	Value	Heartbeat
Searching	0x01	E-Stop Indicated
Stopped	0x04	Nominal / E-Stop Indicated
Operational	0x09	Nominal

Table 1: WES Modes of Operation

6.1. Searching Mode

Searching mode occurs in several cases. If the WES is powered on, but cannot connect to a VSC, the WES LED will blink to show that it is in Searching Mode. This can occur if the VSC is not powered, the WES is not in range to the VSC, or there is a mismatch in network IDs between the WES and VSC.

If the VSC is in Searching mode, then it cannot connect to a WES. This can occur if the WES is not powered, the WES is not in range to the VSC, or if there is a mismatch in network IDs between the WES and VSC.

This is considered an unsafe operating condition because the operator cannot establish a communication link to the vehicle. When the VSC and WES are not connected, the VSC will continue to output the heartbeat message with an indication that the Emergency Stop is active because of the unsafe condition. The Master Enable outputs from the VSC will also be asserted and can be used to prevent motion.

6.2. Operational Mode

Operational Mode is the only state where motion is allowed in the system. When in Operational Mode, the WES and the VSC have established a communication link, and motion is intended. The WES LED will show it is in Operational Mode.

If the VSC is in Operational Mode, the VSC will output the heartbeat message with an indication that the system is operational.

6.3. Error Modes

The WES indicates possible error modes using its two LEDS. The possible error indications are described in the WES data sheet (CDS-020).

6.4. Master Enables

The Master Enable outputs are de-asserted when the system determines that an unsafe condition exists or when the emergency stop has been activated either locally (wired inputs to the VSC) or remotely (from a WES).

The Master Enables will be de-asserted upon the following conditions:

1) The Emergency Stop Button on the WES is activated.
2) The External Emergency Stop Input on the VSC is activated.
3) The Emergency Stop Software Input on the VSC is activated.
4) The VSC loses its connection to the WES.

If the VSC has Master Enable indication asserted, this is considered an unsafe operating condition. It will continue to output the heartbeat message with an indication that the Emergency Stop is active because of the unsafe condition but will return to searching mode as specified. The Master Enable outputs from the VSC will also be de-asserted and should be used to prevent motion.

The Master Enable outputs will only be asserted once the unsafe condition has been acknowledged and corrected.

6.5. VSC LED

The VSC LED indicator is tied to the state of the master enable of the VSC and the connection state of the SRC to the VSC.

LED State	SRCS State
Solid Amber	VSC in bootloader mode
Solid Red	SRC not connected or in estop mode
Blinking Red	SRC connected and VSC estop enabled
Blinking Green	SRC connected and no estops enabled

Table 2: VSC LED States

7. Interfacing using HRI Packet Protocol (USB / RS232)

The command and control communication to the VSC is over the RS232 and USB->Serial interface in the HRI Packet Protocol. The serial format is fixed at 8 data bits, 1 stop bit and no parity with a baud rate of 115200. The VSC USB interface is implemented as a CDC device and on most operating systems it will show up as a serial port (*/dev/tty.usbserial*, */dev/ttyACM0*, etc). An example C application is provided that uses the HRI Packet Protocol to communicate with the VSC over a serial device. The example shows to how provide heartbeat and feedback messages to the VSC while receiving joystick, heartbeat and GPS messages from the VSC. The HRI Packet Protocol is a binary protocol designed with error checking, high efficiency and has a well-defined specification. It is used for all communications between the user and the VSC.

7.1. Data Types

Mode	Size
uint8	0x01
int8	0x01
uint16	0x02
int16	0x02
uint32	0x04
int32	0x04

Table 3: Packet Protocol Data Types

7.2. Packet Structure

Byte Offset	Type	Size	Description
0	uint16	2	Header
2	uint8	1	Message Type
3	uint8	1	Message Length (Size of variable data)
4	Variable	N	Data Packet
N+4	uint16	2	16-Bit Checksum

Table 4: Packet Protocol Structure

7.3. Message Types

The HRI packet protocol contains all of the messages below. The timing of each message that is output from the VSC can be configured using the "Message Control" packet. The default values for the frequency of the messages are shown below.

Type	Description	Direction	Enabled	Frequency
0x20	Heartbeat	From VSC	Yes	20 Hz
0x22	Remote Status	From VSC	No	1 Hz
0x21	Heartbeat	To VSC		20 Hz
0x23	Message Control	To VSC		Aperiodic

Table 5: Packet Protocol Message Types

7.3.1. Heartbeat Message (From VSC)

The heartbeat message from the VSC contains the Emergency Stop indication as well as the current system state.

Byte Offset	Type	Size	Description	Value
0	uint16	2	Header	0x1001
2	uint8	1	Message Type	0x20
3	uint8	1	Message Length	0x06
4	uint8	1	VSC Mode	See state definitions
5	uint8	1	Autonomy Mode	0: User Control 1: Shared Control 2: Autonomous Control
6	uint32	4	E-Stop indication	0 = OK >0 = E-Stop Active (Each bit represents an E-Stop)
10	uint16	2	16-Bit Checksum	See Checksum Reference

Table 6: Packet Protocol Heartbeat Message (From VSC)

7.3.2. Remote Status Message (From VSC)

The Remote Status message from the VSC contains key information pertaining to the connected remote and the status of the link between the VSC and the remote. *NOTE: These values are not cleared when a connection is lost to the remote device. Make sure to use the state in the heartbeat message to indicate whether or not a remote device is connected*.

Byte Offset	Type	Size	Description	Value
0	uint16	2	Header	0x1001
2	uint8	1	Message Type	0x22
3	uint8	1	Message Length	0x06
4	uint8	1	Battery Level	Percentage of battery remaining in 10% increments (0-100%)
5	uint8	1	Battery Charging	0 = Not Charging, 1 = Charging
6	uint8	1	Connection Strength (as perceived by VSC)	0 = Low Connection Strength (intermittent messages, could be disconnected) 1 = Medium Strength 2 = High Strength
7	uint8	1	Connection Strength (as perceived by SRC)	0 = Low Connection Strength 1 = Medium Strength 2 = High Strength
8	uint8	1	RSSI (as perceived by VSC)	Reserved for future use
9	uint8	1	RSSI (as perceived by SRC)	Reserved for future use
10	uint16	2	16-Bit Checksum	See Checksum Reference

Table 7: Packet Protocol Heartbeat Message (From VSC)

7.3.3. Heartbeat Message (To VSC)

The heartbeat message to the VSC contains the Emergency Stop indication from the user. If the User E-STOP Timeout Key is set, the VSC will use this message as a watchdog for the user computer as well. It will indicate an Emergency Stop condition if the user does not periodically send this message (after a 500ms timeout).

Byte Offset	Type	Size	Description	Value
0	uint16	2	Header	0x1001
2	uint8	1	Message Type	0x21
3	uint8	1	Message Length	0x01
4	uint8	1	E-Stop indication	0 = OK >0 = E-Stop Active
5	uint16	2	16-Bit Checksum	See Checksum Reference

Table 8: Packet Protocol Heartbeat Message (To VSC)

7.3.4. Message Control Message (To VSC)

The Message Control message to the VSC allows the user to configure which messages are output from the VSC, and how often. The enabled field determines whether or not the message is transmitted. And the interval is defined as the number of milliseconds between transmissions of the message. All of these settings are persistent in EEPROM, so they only need to be configured once by the user. *NOTE: It is not recommended to disable the heartbeat or joystick messages from the VSC*.

Byte Offset	Type	Size	Description	Value
0	uint16	2	Header	0x1001
2	uint8	1	Message Type	0x23
3	uint8	1	Message Length	0x04
4	uint8	1	Message Type	Which VSC message type to modify
5	uint8	1	Enabled	Whether or not the message is transmitted.
6	uint16	2	Interval	Time between transmissions in milliseconds (20 -> UINT16_MAX)
8	uint16	2	16-Bit Checksum	See Checksum Reference

Table 9: Packet Protocol Heartbeat Message (To VSC)

7.4. 16-bit Checksum Reference

The 16-bit Checksum used is a variation of the Fletcher 16 checksum for computing a position-dependent checksum devised by John G. Fletcher at Lawrence Livermore Labs in the late 1970s. The objective of the Fletcher checksum was to provide error-detection properties approaching those of a cyclic redundancy check but with the lower computational effort associated with summation techniques. The algorithm to calculate the checksum is shown below.

```
1.  uint16_t checksum16( uint8_t* data, int count )
```

```
2.  {
3.    uint16_t sum1 = 0;
4.    uint16_t sum2 = 0;
5.    int index;
6.
7.    for( index = 0; index < count; ++index )
8.    {
9.      sum1 = (sum1 + data[index]) & 255;
10.     sum2 = (sum2 + sum1) & 255;
11.   }
12.
13.   return (sum2 << 8) | sum1;
14. }
```

Figure 3: Checksum Reference

8. Interfacing using CAN-J1939 Protocol

The CAN Protocol is a binary protocol designed to be compatible with the J1939 specification. It is used for all communications between the user and the VSC.

8.1. Packet Structure

The SRCS uses the SAE J1939 basic joystick message to transfer information about the measured status of the X, Y and Z-axis of a joystick, and the state of buttons. The SRCS uses custom SAE J1939 messages to transfer the heartbeat and key-value pair information.

8.2. Message Types

Type	Description	Direction	Frequency
0x0CFD E801	Heartbeat - J1939 Custom Message	From VSC	10 Hz

Table 10: Message Types

8.2.1. Heartbeat Message (From VSC)

The heartbeat message from the VSC contains the Emergency Stop indication as well as the current system state.

Byte Offset	Size	Description	Value
0	1	VSC Mode	See state definitions
1	1	Autonomy Mode	0: User Control 1: Shared Control 2: Autonomous Control
2	4	E-Stop indication	0 = OK >0 = E-Stop Active (Each bit represents an E-Stop)

Table 11: Heartbeat Message (From VSC)

9. Troubleshooting

Here is a list of the most common problems users are reporting, with a solution.

Issue	Symptom	Solution
Not receiving data from the VSC.	If the color of the LED is ORANGE, this means that the VSC was reset with the bootloader indicator set.	Verify the state of the Emergency Stop input on the VSC. This is used to tell the VSC to go into bootloader mode on boot.

10. Limited Warranty

All products sold by Humanistic Robotics, Inc are subject to the warranty provisions of the Humanistic Robotics Order Confirmation terms and conditions and are warranted against defects in material and workmanship for a period of one (1) year from the date of shipment. If you believe any Humanistic Robotics, Inc product you have purchased has a defect in material or workmanship or has failed during normal use within the warranty period, please contact Humanistic Robotics, Inc for assistance. If product repair or replacement is necessary, the Customer will be solely responsible for all shipping charges, freight, insurance and proper packaging to prevent breakage in transit, whether or not the product is covered by this warranty.

This warranty does not apply to defects resulting from any Customer actions, such as mishandling, improper interfacing, operation outside of design limits, misapplication, improper repair, or unauthorized modification. No other warranties are expressed or implied. Humanistic Robotics, Inc specifically disclaims any implied warranties of merchantability or fitness for a specific purpose and all warranties arising from course of dealing and/or trade usage. Humanistic Robotics, Inc.'s liability shall be limited to the actual purchase price of any defective unit or units of equipment to which a claim is made, and shall in no event include the Customer's manufacturing costs, lost profits or goodwill, or any other direct, indirect, special, incidental, consequential or punitive damages whether based on contract, tort or other legal theory. Humanistic Robotics, Inc shall not be liable for normal manufacturing defects or customary variances from specifications.

Products sold by Humanistic Robotics, Inc are not designed, intended or authorized for use in applications intended to sustain or support life, in any nuclear facilities or any other application where the failure of the product could create a situation where catastrophic property damage, personal injury or death may occur. In the event that the Customer purchases or uses any Humanistic Robotics, Inc products for any such unintended or unauthorized application, the Customer shall indemnify and hold harmless Humanistic Robotics, Inc and its officers, directors, employees, agents, affiliates, successors and assigns against all claims, costs, damages and expenses (including reasonable attorneys' and expert witness' fees) arising out of or in connection with, directly or indirectly, any claim for property damage, personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Humanistic Robotics, Inc was negligent regarding the design or manufacture of the subject product.

11. Revision History

Version	Date	Changes
-01	8/10/14	Initial Release

Humanistic Robotics, Inc.
111 South Independence Mall East
Suite 1010
Philadelphia, PA 19106
1-267-515-5880
www.humanisticrobotics.com